Configuración de la Autenticación TACACS+ en CIMC con el Servidor ISE

Contenido

Introducción

Este documento describe la configuración de la autenticación de Sistema de control de acceso del controlador de acceso de terminal Plus (TACACS+) en Cisco Integrated Management Controller (CIMC).

TACACS+ se utiliza habitualmente para autenticar dispositivos de red con un servidor central. Desde la versión 4.1(3b), Cisco IMC admite la autenticación TACACS+. La compatibilidad con TACACS+ en CIMC facilita el esfuerzo de administrar varias cuentas de usuario que tienen acceso al dispositivo. Esta función es de ayuda para cambiar periódicamente las credenciales del usuario y gestionar las cuentas de usuario de forma remota.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de gestión integrada de Cisco (CIMC)
- Terminal Access Controller Access-Control System Plus (TACACS+)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCSC-C220-M4S
- Versión de CIMC: 4.1(3 ter)
- Cisco Identity Services Engine (ISE) versión 3.0.0.458

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración del lado del servidor TACACS+ para asociación de privilegios

El nivel de privilegio del usuario se calcula en función del valor de par **cisco-av-**configurado para ese usuario. Se debe crear un **par** cisco-av en el servidor TACACS+ para y los usuarios no pueden utilizar ningún atributo TACACS+ predeterminado. Las tres sintaxis como se muestra a continuación son compatibles con el atributo **cisco-av-pair**

Para el privilegio **de administración**:

```
cisco-av-pair=shell:roles="admin"
```

Para el privilegio **de usuario**:

```
cisco-av-pair=shell:roles="user"
```

Para el privilegio **de sólo lectura**:

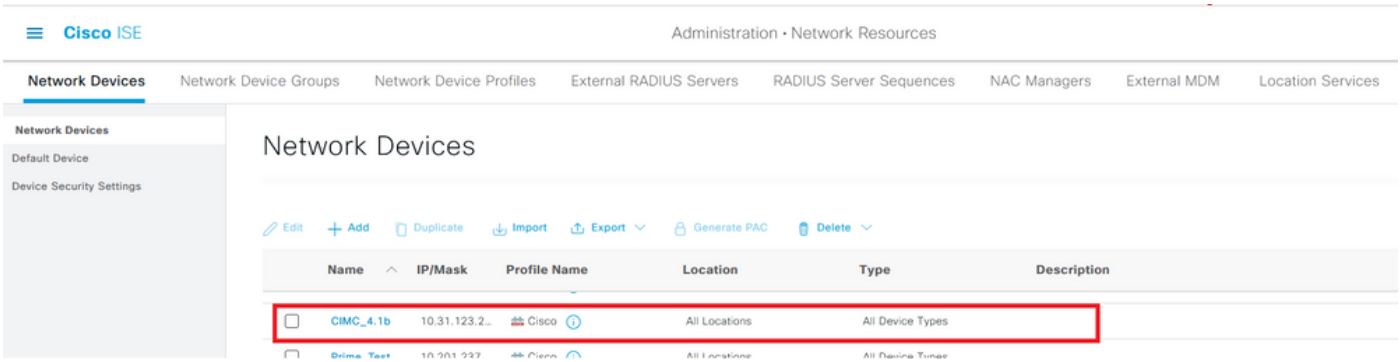
```
cisco-av-pair=shell:roles="read-only"
```

Para admitir otros dispositivos, si es necesario agregar otras funciones, se pueden agregar con una coma como separador. Por ejemplo, UCSM admite **aaa**, por lo que **shell:roles="admin,aaa"** se puede configurar y CIMC acepta este formato.

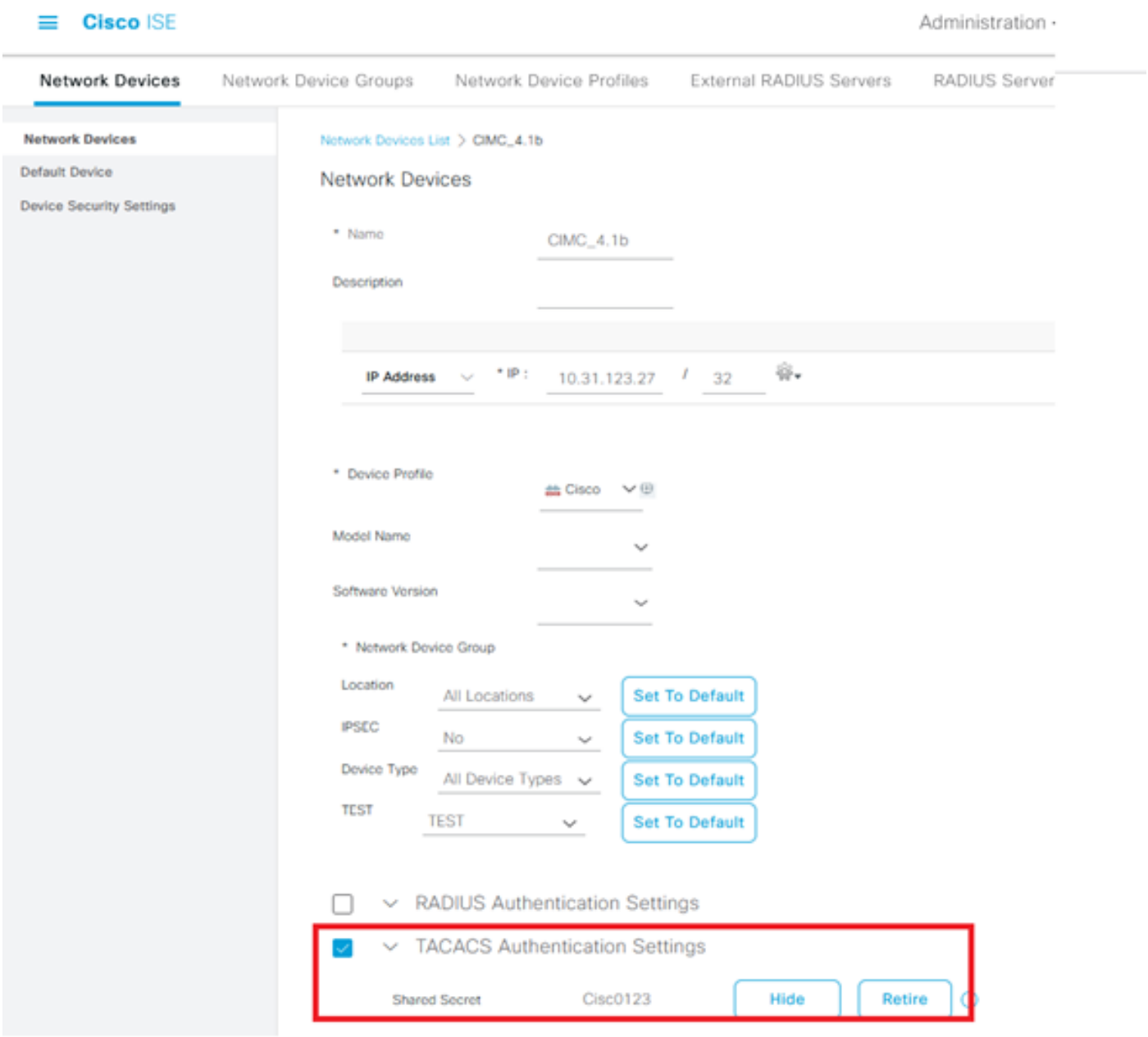
> **Nota:** Si **cisco-av-pair** no está configurado en el servidor TACACS+, entonces un usuario con ese servidor tiene un **privilegio de sólo lectura**.

Requisitos de configuración de ISE

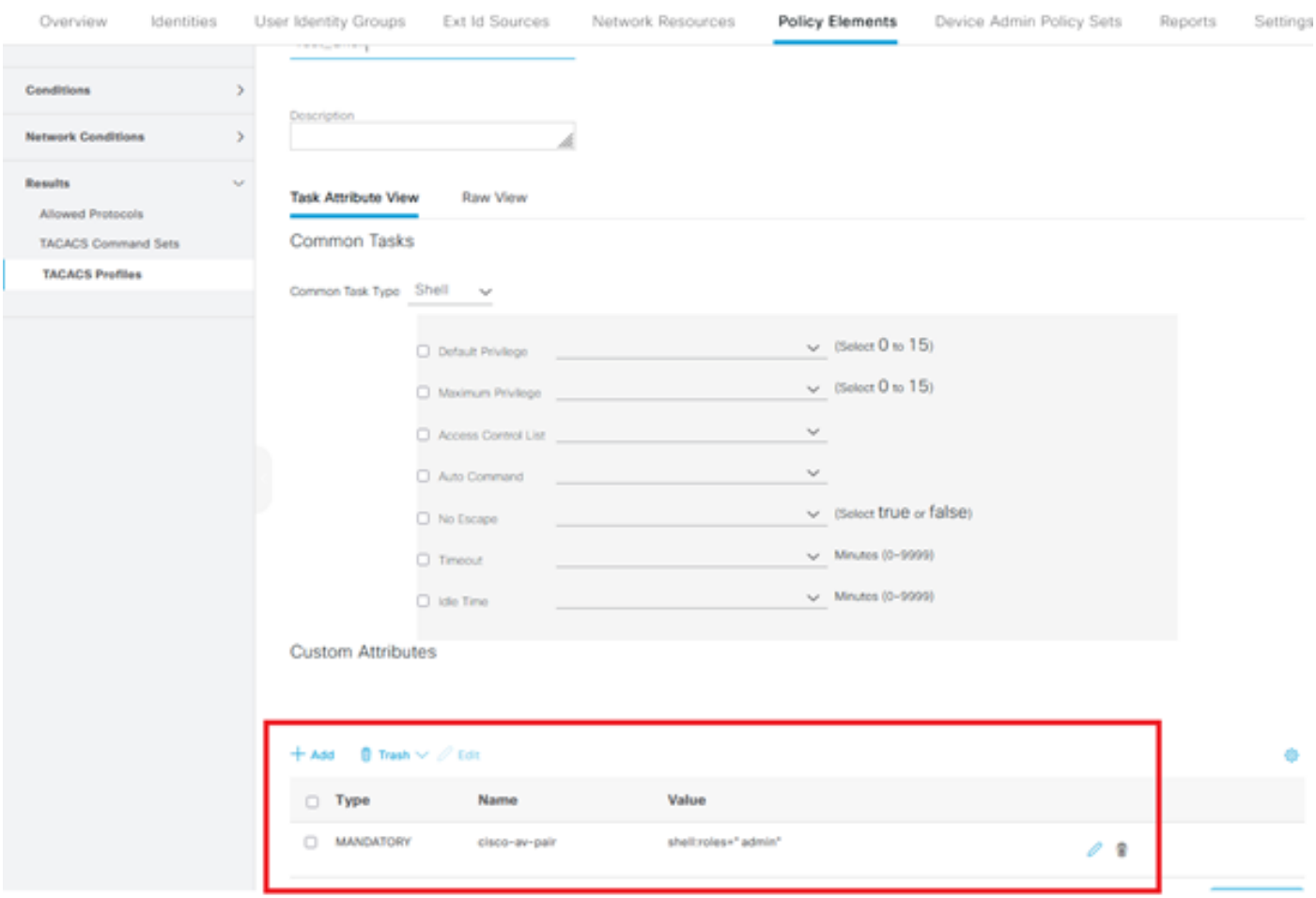
Se debe permitir la IP de administración del servidor en los dispositivos de red ISE.



La contraseña secreta compartida se ingresará en CIMC.



Perfil de Shell con el atributo **cisco-av-pair** con permisos de administrador.

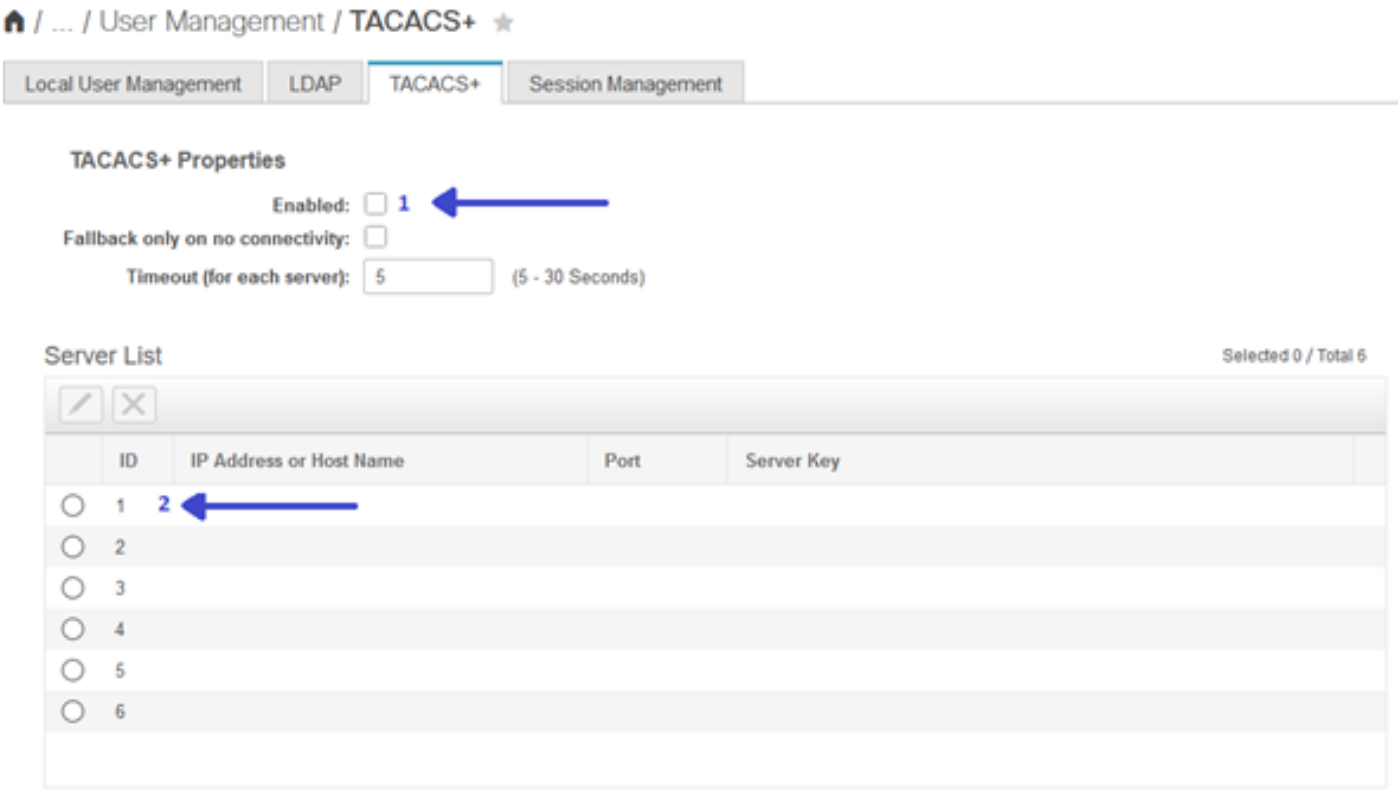


Configuración TACACS+ en CIMC

Paso 1. Vaya a **Admin > User Management > TACACS+**

Paso 2. Active la casilla de verificación para activar **TACACS+**

Paso 3. Se puede agregar un nuevo servidor en cualquiera de las 6 filas especificadas en la tabla. Haga clic en la fila o seleccione la fila y haga clic en el botón **editar** de la parte superior de la tabla, como se muestra en esta imagen.

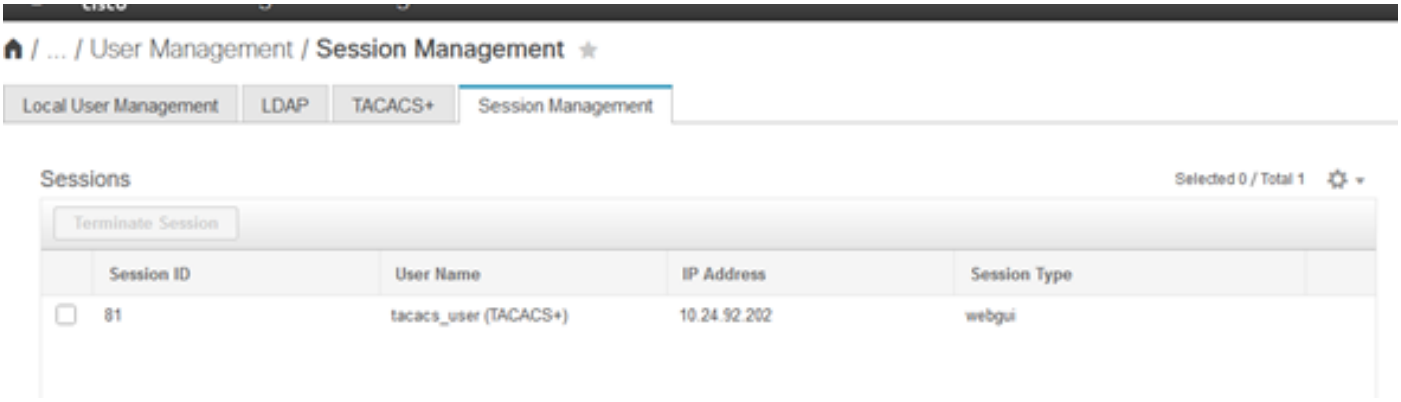


Nota: En el caso de que un usuario haya habilitado el repliegue de TACACS+ en ninguna opción de conectividad, CIMC aplica que la primera prioridad de autenticación siempre se debe establecer en TACACS+; de lo contrario, la configuración de repliegue podría volverse irrelevante.

Paso 4. Rellene la dirección IP o el nombre de host, el puerto y la clave de servidor/secreto compartido y **guarde** la configuración.

Cisco IMC admite hasta seis servidores remotos TACACS+. Una vez que un usuario se ha autenticado correctamente, el nombre de usuario se agrega con (TACACS+).

Esto también se muestra en la Administración de sesiones



Verificación

- Se puede configurar un máximo de 6 servidores TACACS+ en el CIMC.
- La clave secreta asociada al servidor puede tener una longitud máxima de 64 caracteres.
- El tiempo de espera se puede configurar entre 5 y 30 segundos (que se evalúa como máximo en 180 segundos para estar en línea con LDAP).
- Si un servidor TACACS+ necesita utilizar el nombre de servicio para crear el **par cisco-av**, los usuarios deben utilizar **Iniciar sesión** como nombre de servicio.
- No hay soporte de pelirroja para modificar las configuraciones.

Verificar la configuración desde CLI en CIMC

- Verifique si TACACS+ está habilitado.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- Verifique los detalles de la configuración por servidor.

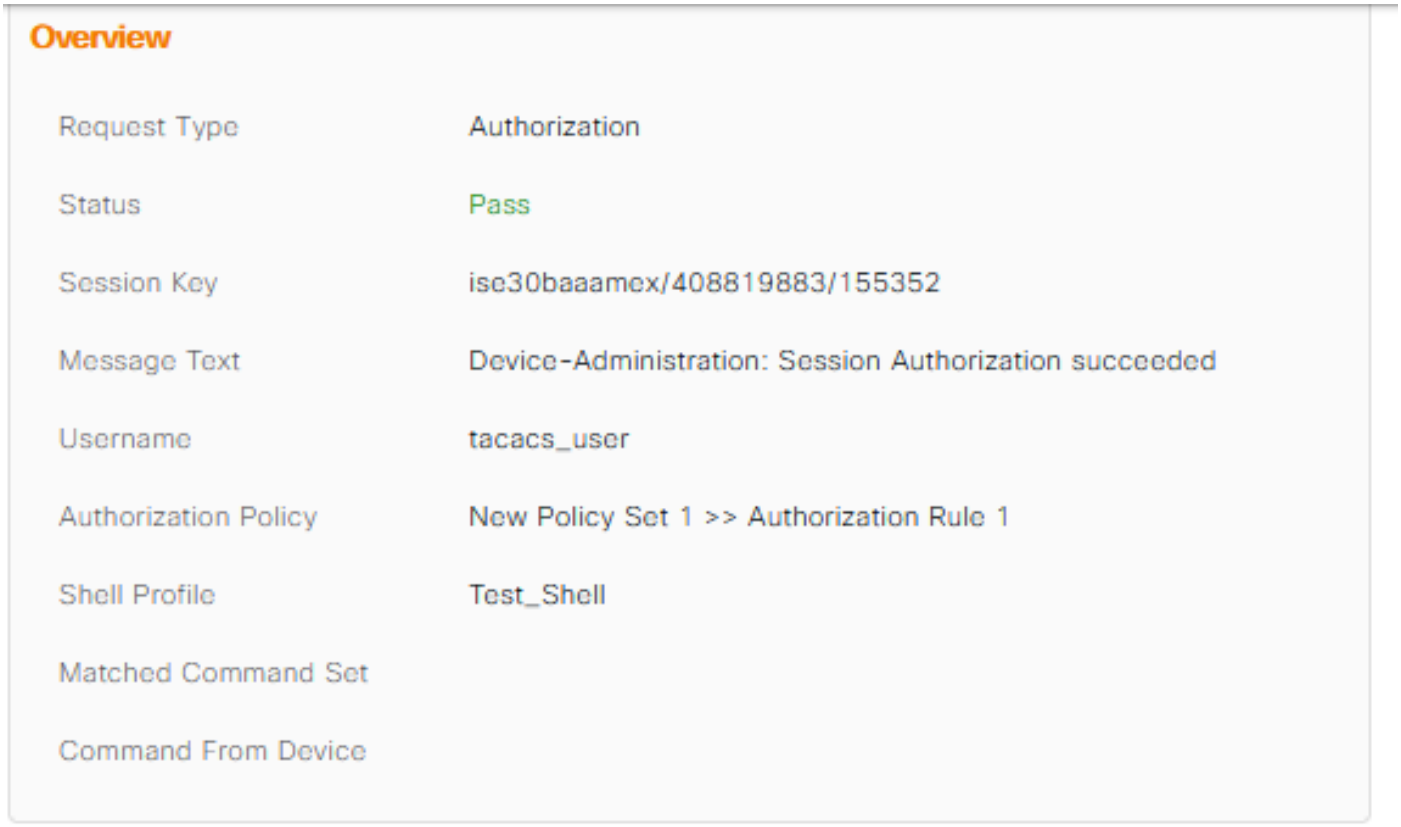
```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: ******
Server Port: 49
```

Troubleshoot

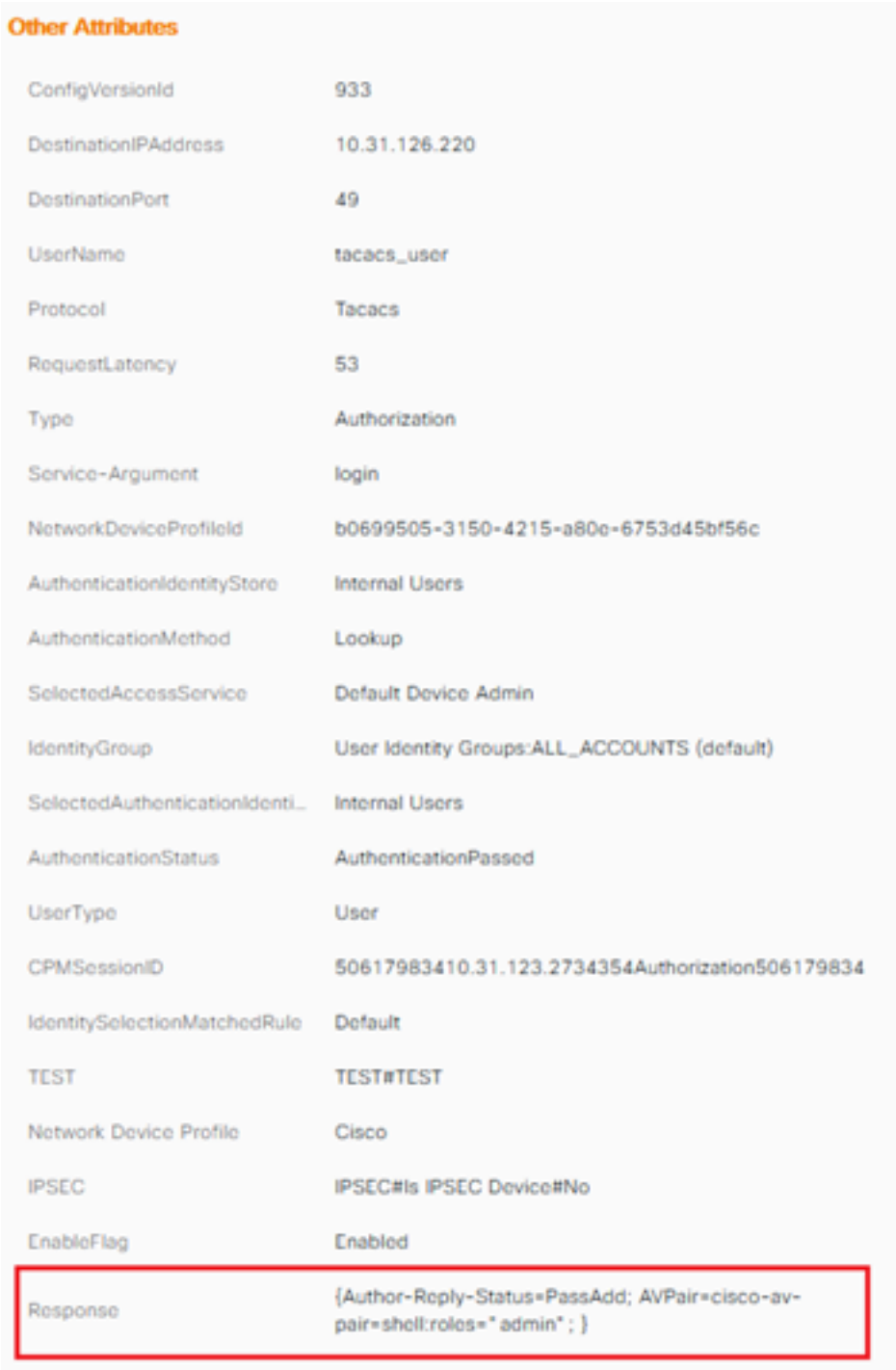
- Asegúrese de que la IP del servidor TACACS+ esté accesible desde el CIMC y que el puerto esté configurado correctamente.
- Asegúrese de que el **par cisco-av** esté configurado correctamente en el servidor TACACS+.
- Compruebe si el servidor TACACS+ es accesible (IP y puerto).
- Asegúrese de que la clave secreta o las credenciales coincidan con las configuradas en el servidor TACACS+.
- Si puede iniciar sesión con TACACS+ pero sólo tiene permisos **de sólo lectura**, verifique si cisco-av-pair tiene la sintaxis correcta en el servidor TACACS+.

Solución de problemas de ISE

- Verifique los registros Tacacs Live para uno de los intentos de autenticación. El estado debe ser **Pass**.



- Verifique que la respuesta tenga el atributo **cisco-av-pair** correcto configurado.



Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

Información Relacionada

- Autenticación TACACS+ Cisco UCS-C
- Soporte Técnico y Documentación - Cisco Systems
- Configuración de ISE 2.0: Autorización de Autenticación y Comando TACACS+ de IOS basada en la pertenencia al grupo AD